PM-ISE Workshop for Information Sharing and Safeguarding Standards (WIS^3)

Appendix B – WIS3 Breakout Track 2

Identity and Access Management Across Government

Panelists

Name	Organization	Role / Presentation
Dave Chesebrough	Association For Enterprise Information (AFEI)	Moderator
Chris Louden	Protiviti	Attribute Governance and the Backend Attribute Exchange
Rebecca Nielsen	Booz Allen Hamilton	Industry Perspective Regarding Gaps in Achieving IdAM Across Government
Scott McGrath	Organization for the Advancement of Structured Information Standards (OASIS)	Security Assertion Markup Language (SAML) & XACML
John Ruegg	Los Angeles County Information Systems Advisory Body	Global Federated Identity and Privilege Management (GFIPM) & National Information Exchange Federation (NIEF)

Observations: The key elements of federating Identity and Access Management (IdAM) seem to aggregate into distinct groupings: policy, governance. funding, terminology and implementation.

Status on Backend Attribute Exchange (BAE) v2 was briefed. The DHS pilot substantially matured the technical specifications. A basic set of agreed-upon attributes is needed for BAE to be usable between entities. An Access Control Attribute Governance WG (ACAG WG) is being established with a focus on governance, coordination of semantics, syntax, and protocol. The ACAG WG will coordinate a common language and understanding of access control attributes across the federal government (alignment with NIEM).

An industry perspective on the gaps between federated identity protection and management policy and requirements which industry partners receive for implementation of federal identity systems was provided. Improvements need to be made in synchronization of federal policies, procurement and acquisition strategies. A perception that the Government has a penchant for requiring certain capabilities and then ignoring those requirements when selecting vendors/contractors was acknowledged by attendees. If Government expects industry to provide a specific capability, there needs to be a market to sell that capability into. This is also true of level 2 and 3 credentials. Even where clear guidance regarding federated

interoperable credentials exists, agencies continue to implement solutions that require application specific credentials, impacting market demand. A related recommendation was made to work on enabling applications to accept credentials. In addition, a lack of common terminology and perceived lack of implementation funding were cited as gaps. Recommendations include establishment of a common governance structure connecting all stakeholders; applying policy requirements to logical vice physical access control, especially for logical access to information systems with a broad user base across government and industry; and creation of implementation guides that can be used across Federal agency information systems to encourage interoperability.

Interoperable, federated identity management frameworks across enterprise architectures were the next topic. With a set of interoperable standards, each standard permits the use of the others, depending on the conformance of vendors. With regard to infrastructure, there was discussion about developing a frame and model for governance of federations and a need for an infrastructure for access behaviors and access controls. Use of XACML to enable federated identity as a standard for access control was briefed. A major point was made that an adoption strategy for federated identity management is necessary for target architectures and that incremental accomplishments and implementation should be aligned with an objective adoption strategy that is stable over a long period such that progress can be evaluated against it.

Federated identity management and its implications to invoke a single sign-on capability across the NIEF/GFIPM was the next topic. Numerous implementation challenges have been identified, including governance and semantics. Attendees were told of GFIPM's attempt to use attributes in their work and the eventual move to the use of rules to define access because of the complexity of attributes and the lack of meaningful semantic standards for attributes, leading to varying definitions and applications. Conditional attributes based on specific roles were recommended for consideration.

Discussion was also driven towards sharing in the context of communities of interest. Different approaches to access control (attribute-based, role/function-based, context-based) will have implications for approaches to identity frameworks. With regard to sharing data it was expressed that it can viewed in terms of what one needs to know and when one needs to know it and obtaining access based on attribute, role or context.

There was significant dialogue on governance in the context of access to certain classes of information. Risk management and privacy are also important elements. Attendees from the FBI spoke about the need to make sure that safeguarding was not ignored. The threat is ever present and sharing must be balanced with the risk and context. Comments were made in the context of an information sharing event and how dissemination rules from the information owner must follow that information when it is shared. The risk dimension was also discussed in the context of the decision to share and be a part of the assessment of sharing or not sharing.

Some commented on the need for ‘design patterns’, reuse of solutions, and access to use cases and user stories so that adopters can make trade-off decisions. There were also comments relating to understanding the difference between tagged data and meta-data, and how those are quite different in implementation. Also discussed were roles and attributes for given use cases, collecting and making available lessons from successful roll-outs. A suggestion was made that a “sandbox” for security and identity management might be useful so that use cases, real problems, and successful solutions can be tried before adoption.